Is Trident Crippled?

John Ainslie

John Ainslie, the Coordinator of Scottish CND, sent this paper to the Defence Select Committee after he gave evidence to their inquiry on nuclear weapons. It develops some of the issues raised in his authoritative study 'The Future of the British Bomb' *(see* Spokesman 92*).*

In 1988, an Audit Office report into the Trident programme said:

> 'proving the effectiveness of the system for UK purposes is dependent on the production in the UK of software for targeting, modelling and effectiveness assessment'.

The report pointed out that at the time the Director General Strategic Weapon Systems was having difficulty recruiting suitable staff. In 1994, the Defence Minister said that software development work had been completed using a mix of internal expertise and specialist contractor support.

Reliance on US software

The designers of the Trident D5 adopted a systems-wide approach to meet the accuracy specifications of the missile. They studied and modelled each factor that could reduce accuracy and created a substantial complex of software, computer models and data. These are not static but are regularly updated. While the United Kingdom does produce some software for the British Trident system, much of it is of US origin.

The Applied Physics Laboratory of John Hopkins University in Maryland (APL) evaluates the UK Trident missile system. APL designed the systems used to monitor missile tests and they analyse all British tests. Additional analysis is carried out by Charles Stark Draper Laboratories, who make the missile guidance system.

The Trident Fire Control hardware is manufactured by General Dynamics Defense Systems (GDDS). The US Navy regularly places contracts with GDDS for updates of software for the UK fire control system.

K Department of the Naval Surface Warfare Center at Dahlgren in Virginia develops and tests the targeting and fire control software for Trident. The contractor who supports K Department is required to –

'coordinate the development of fire control specifications for the United States and United Kingdom submarine-launched ballistic missile (SLBM) systems and support specification testing … perform the verification, acceptance, static and/or dynamic testing tasks for up models including Fire Control support software, United Kingdom reference/simulation models, US/UK targeting models and SLBM general purpose tools'.

The models referred to are at the heart of the Trident system. They are used for shore-based targeting and performance assessment. In addition parts of these models are integrated into the fire control software on Trident submarines.

In the British software facility programmers maintain, update and modify US codes and models for inclusion in the suite of codes for the UK Trident system.

Validation of US software in the United Kingdom

When asked about the verification of US fire control software, Defence Minister Des Browne said,

'Each new release of Trident fire control software is certified by the US Government under the terms of the Polaris Sales Agreement (as amended for Trident). Under the agreement, the UK has the capability to validate the software models for software performance and verify that the findings are correct. This is undertaken and independently verified by UK experts to ensure the software meets our requirements before being issued to Royal Navy submarines.'

Adam Ingram, junior Defence Minister, was asked about US software for the shore-based system and said,

'The UK shore-based target planning system for Trident is validated through a range of UK and US research programmes. UK experts then independently verify the system against requirements before issuing it to Royal Navy submarines'.

Work on software for Trident is carried out in the Corsham Computer Centre also referred to as the Corsham Software Facility. This is an underground complex close to Basil Hill Barracks in Wiltshire. Mass Consultants Ltd manage the IT system in the centre, on behalf of the Strategic Systems Integrated Project Team. Analysts who assess the performance and effectiveness of Trident use the IT facilities in centre.

The one company in the United Kingdom with expertise in analysing submarine-launched ballistic missile trajectories was Hunting Engineering Ltd. The company changed its name to INSYS and then to Lockheed Martin UK. They now are a subsidiary of the US firm with the main Trident contract.

Some of the validation will be carried out at Corsham but other work is probably contracted out to Lockheed Martin UK.

Removal of classified items from US software

British experts will be hampered in their attempt to validate the software by the constraints of US security restrictions. The Joint Strike Fighter deal showed the difficulties of purchasing equipment which is dependent on sensitive American software. In the case of Trident the United States does supply the software codes,

but not in their original complete form.

A substantial proportion of US nuclear targeting information is classified so that only US citizens can see it. The Chief of Staff has issued a directive specifying how classified items should be removed from nuclear targeting information, in a process called sanitising, before it is handed to the Corsham Computer Centre, the London targeting centre or the British contingent at Strategic Command in Omaha.

The contractor at Dahlgren has to check that any software handed to Britain has been sanitized, as part of the Quality Assurance (QA) process –

'For the QA of UK models, the contractor shall analyse the software, data and documentation to verify that all US-only items have been removed.'

This implies that the process is as follows:
1. US contractors produce software items for the US Trident system
2. US-only items are removed from the code, data tables and instruction manuals
3. A US contractor verifies that these items have all been removed
4. The cut-down software is handed to the Corsham Computer Centre
5. Corsham and Lockheed Martin UK check that the software works
6. The software is issued to submarines, the London Targeting Centre and/or the Corsham Computer Centre as appropriate

Implications for the independence of UK Trident

From the perspective of Washington it would be desirable to create the impression that Britain can use Trident independently while at the same time maintaining a veto over actual use. One particular concern will be the potential for Britain to launch 144 nuclear warheads at the United States.

How could the software stop a Trident launch?

General restrictions
Preventing the use in all circumstance except tests, or preventing the missiles from being fired westwards, towards the United States from the normal patrol areas, should be possible.

Restricting the system to only NATO or joint US/UK plans
The fire control system can probably distinguish an independent British plan from a NATO or Anglo-American plan. Any allied or joint plan would have to be deconflicted. This is a process of integrating two plans to ensure that they do not undermine each other's effectiveness. For example debris in the fallout cloud from the explosion of a British nuclear explosion could cripple a US nuclear weapon and prevent it from detonating. For reasons of complexity and classification it is not possible to run a US attack plan through the British computer system. Deconflicting can only be carried out by running the British plan through the main US nuclear planning system at Strategic Command in Omaha. This deconflicting

process is likely to leave a trace in the data which could be detected by the fire control software on the submarine. If the software can distinguish a Nato plan from an independent one, then it could possibly prevent the independent plan from being implemented.

Restricting use by manipulating weather data

A NATO or Anglo-American plan would probably use US weather data. The fire control system requires details of weather over the target area if it is to achieve the desired level of accuracy. For an attack on Russia a large amount of data is required on wind speed and air density at various altitudes. This data has to be transmitted over very low frequency (VLF). It is compressed and formatted in the US into Ballistic Parameters (Balpars). These are transmitted every 12 hours. There are similar mechanisms for producing detailed weather data when Trident is being retargeted against specific targets. It is possible that information could be contained within Balpars or other weather data that would have the effect of switching on or off the UK fire control system.

If the US tampered with the software, would we find out?

The US Navy asked Mountain State Information Systems to check the security of the US Trident software. The company's description of this work reveals that this was a complex task for which they had to develop new techniques. This suggests that if the US programmers tried to hide commands within the software it would not be easy for British experts to find them.

The task is made particularly difficult because of the holes in the code, data and manuals where items have been removed for reasons of security. This means that there will be parts of the UK software which do not make sense. But the US manufacturers will not be able to explain the anomalies because the missing material is classified.

As the software has a mixture of cut-down US components and British elements it will be a difficult task to get it to work. This is probably the main focus of the British software effort. Checking to see if the Americans have crippled the code is probably not a priority.

This does not establish that the software has been crippled, but does suggest that it could be. The only way that Britain can guarantee that the Trident software has not been modified would be to produce it all ourselves. But we do not currently have the expertise to do this.

References available on request.